DETAILED ACTION

Claims 1-43 are pending in the amendment 06/07/10.

Below, Examiner has pointed out particular references contained in the prior art(s) of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claims, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully each reference in its entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. **Claims 1, 9, 15-23, 29, 30, and 35-43** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Baker (US 6,775,657),** hereafter "Baker", in view of **Kaashoek et al. (US 7278159), hereafter "Kaashoek."**

Considering **Claims 1 and 43,** Baker discloses a method of monitoring propagation of viruses by a first host within a network of hosts (abstract), the method

comprising the following steps carried out by the first host: establishing a record which is at least indicative of identities of destination hosts within the network to whom data has been sent by the first host (Fig. 2, column 4- lines 32-58); during a first time interval, comparing (a) identities of destination hosts identified in requests to send data from the first host (column 5- lines 10-29) and (b) identities of destination hosts identified in the record (column 5- lines 10-29); transmitting all requests to send data (column 5- lines 21-38).

Baker does not explicitly disclose storing in a buffer data relating to requests which identify a destination host not in the record. Baker teaches that if a request identifies a host not in the record, the network activity is subjected to intrusion detection services. This suggests that the destination host would be stored. Kaashoek discloses storing in a buffer data relating to requests which identify a destination host not in the record (column 4- lines 34-53).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Baker by storing in a buffer data relating to requests which identify a destination host not in the record as taught by Kaashoek in order to analyze the data collected over a period of time and if necessary raise an alarm (Kaashoek- column 4- lines 50-53)

Considering **Claims 29, 41, and 42,** Baker discloses a method of operating a first host within a network of a plurality of hosts (abstract), said method comprising the following steps carried out by a first host: over the course of a first time interval, monitoring creation of sockets within the first host to identify destination hosts identified therein (Fig. 2, column 4- lines 32-58); comparing identities of destination

hosts monitored during the first time interval with destination hosts in a record (column 5- lines 10-29).

Baker does not explicitly disclose storing data from all sockets which identify monitored destination hosts not in the record.

Kaashoek discloses storing data from all sockets which identify monitored destination hosts not in the record (column 4- lines 34-53).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Baker by storing in a buffer data relating to requests which identify a destination host not in the record as taught by Kaashoek in order to analyze the data collected over a period of time and if necessary raise an alarm (Kaashoek- column 4- lines 50-53).

Considering **Claim 8,** the combination discloses the stored data is offered in a buffer and includes a copy of a socket created to send data in accordance with a request (Kaashoek- Fig. 4).

Considering **Claims 9 and 30,** the combination discloses the socket enables identification of at least one application program at whose behest the socket is created (Barrett- column 11- lines 30-41).

Considering **Claim 15,** the combination discloses the step of monitoring the rate of increase in the size of the buffer, and in the event that the rate of increase in the size of the buffer exceeds a predetermined rate, generating a warning (Kaashoek- column 4- lines 50-53).

Considering **Claim 16,** the combination discloses monitoring the increase in the size of the buffer per time interval, and in the event that the increase in the size of the

buffer in any given time interval exceeds the predetermined size, generating a warning (Kaashoek- column 4- lines 50-53).

Considering **Claim 17,** the combination discloses the step of monitoring the size of the buffer, and in the event that the buffer exceeds a predetermined size for a predetermined number of successive time intervals, generating a warning (Kaashoek- column 4- lines 50-53).

Considering **Claim 18,** the combination discloses at least one parameter selected from the group consisting of: number of destination hosts in the record; threshold number of requests identifying destination hosts not in the record and defining a state of viral infection, is varied with time (Fig. 2, column 4- lines 32-58, Kaashoek- column 4- lines 50-53).

Considering **Claims 19 and 22,** the combination discloses at least one parameter is varied as a function of the time of day (Fig. 2, column 4- lines 32-58, Kaashoek- column 4- lines 50-53).

Considering **Claim 20,** the combination discloses at least one of the parameters is varied in response to a perceived threat level (Fig. 2, column 4- lines 32-58, Kaashoek- column 4- lines 50-53).

Considering **Claim 21,** the combination discloses at least one of the parameters is changed between a first set of values and a second set of values at a predetermined rate (Kaashoek- Fig. 4).

Considering **Claim 23,** the combination discloses at least one parameter selected from the group consisting of: number of destination hosts in the record; threshold number of requests identifying destination hosts not in the record and defining a state

of viral infection, is determined by performing an automated search on a set of data indicative of normal network traffic (Kaashoek- Fig. 4).

Considering **Claims 35 and 38,** the combination discloses the step, in the event that the number of socket data items stored exceeds a predetermined value, of storing outgoing packets from the first host (Kaashoek, column 4- lines 34-53).

Considering **Claim 36 and 39,** the combination discloses packets having a designated destination IP address is stored (Kaashoek, column 4- lines 34-53).

Considering **Claim 37 and 40,** the combination discloses the step of establishing the predetermined IP address from the stored socket data (Kaashoek, column 4- lines 34-53).

Response to Arguments

Applicant's arguments filed 6/7/2010 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Baker (US 6,775,657).

Allowable Subject Matter

Claims 2-8, 10-14, 24-28 and 31-34 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to RANDAL D. MORAN whose telephone number is (571)270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Randal D. Moran/
Examiner, Art Unit 2435

/Beemnet W Dada/
Primary Examiner, Art Unit 2435

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435